学校编码：10384
学号：23020071151307
分类号_____密级_____
UDC_____

厦门大学

硕 士 学 位 论 文

Linux 下基于高速报文捕获平台的 DDoS 入侵检测系统

The DDoS Intrusion Detection System Based on High-speed Packet Capture Platform of Linux

许晓晨

指导教师姓名：黎忠文 教授

专 业 名 称：计算机系统结构

论文提交日期：2010 年 5 月

论文答辩时间：2010 年 月

学位授予日期：2010 年 月

答辩委员会主席：_____

评 阅 人：_____

2010 年 5 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（兼容 Libpcap 的 Linux 千兆网卡加速中间件 NCTI 科技计划项目）课题（组）的研究成果，获得（兼容 Libpcap 的 Linux 千兆网卡加速中间件 NCTI 科技计划项目）课题（组）经费或实验室的资助，在（厦门大学计算机系网络安全实验室）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：许晓东

2010年6月2日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：许晓敏

2017 年 6 月 2 日

摘　　要

在百兆环境下使用的 Linux 系统自带的 Libpcap 分组捕获函数库已经不能继续满足人们的需求，因为其“每包驱动”的特性在千兆环境下产生大量中断，造成中断淹没和丢包率急剧上升，引起系统瓶颈，若系统不改进，则会影响其他网络应用例如入侵检测系统、网络协议分析和网络防火墙的效率，变成千兆网络普及的阻碍。因此如何在千兆网络环境下实现线速的报文捕获以及上层的安全应用，一直是研究的热点。基于此，作者开展了本项研究，包括两方面内容。一方面，针对线速报文捕获问题，本文基于 Linux 平台，用零拷贝和内存映射等方法设计和实现了一个高速报文捕获平台，具有线速报文捕获、CPU 占用率低和与 Libpcap 兼容的特点。另一方面，考虑到大多数现有的抗 DDoS 攻击的工具主要关注于入侵的检测和发现新的入侵特征，在实际应用时存在攻击检测滞后的问题，在高速报文捕获平台上，设计和实现了能及时发现攻击并且能及时进行防御的入侵检测系统。

本文主要工作如下：

1、对 Linux 的系统内核、网络协议、自带的传统数据报文捕获平台 Libpcap，以及 Linux 下 Intel 千兆网卡的驱动程序进行了深入的分析。

2、用内存映射和中断节制机制等方法实现了一个新的数据捕获平台，本平台可以在千兆网络环境下线速地捕获数据并且兼容传统的 Libpcap 平台。

3、对 DDoS 攻击的特征和现有的入侵检测方法进行了深入分析。提出了新的 DDoS 攻击检测算法，并在高速数据捕获平台上实现了基于该算法的 DDoS 入侵检测系统。

4、对数据捕获平台和入侵检测系统进行了性能测试，验证了其可靠性和有效性。

关键字：数据捕获，网卡，线速，DDoS 攻击，入侵检测

Abstract

The packet capture library of Libpcap in Linux that was used under Fast network can no longer meet people's needs, since its "every package-driven" features. Large numbers of interrupt were produced in Gigabit environment, leading to system bottlenecks such as livelock and high rate of packet loss. If the system does not improve, the efficiency of network applications such as intrusion detection systems, network protocol analysis and network firewall will be affected and the gigabit network's popularity will also be hindered.

Therefore, how to achieve wire-speed packet capture system and top security applications in gigabit network has been a hot point of research. Based on this, the authors carried out this study, including the two aspects. First, contrary to the problem of wire-speed packet capture, this paper designed and implemented a high-speed packet capture platform using the theory of zero-copy and memory mapping in Linux. This platform can capture packets in wire-speed, has a low CPU occupancy rate and is compatible with Libpcap. On the other hand, because most existing anti-DDoS attack tools were focused on intrusion detection and discovery of new intrusion features, it has the problem of detection time delay in the practical application. We design and implement an intrusion detection system that can detect and defense the attack in time under the high-speed packet capture platform.

Main tasks:

1、Analyzed the kernel, the network protocols, the traditional data packet capture platform Libpcap of Linux, and the driver of Intel Gigabit Ethernet.

2、Implemented a high-speed packet capture platform using the theory of zero-copy and memory mapping in Linux. This platform can capture packets in wire-speed, has a low CPU occupancy rate and is compatible with Libpcap.

3、Analyzed the existing DDoS intrusion detection methods. Proposed a new DDoS attack detection algorithms, and implement the algorithms in high-speed packet capture platform.

4、Test the performance of the packet capture platform and intrusion detection system and verify its reliability and validity.

Key Word：Data Capture; NIC; Wire-speed; DDoS Attacks；Intrusion Detection.

目　　录

Content